SiteGuarding.com

Professional Web Security Services

# ANTIVIRUS SITE PROTECTION (by SiteGuarding.com)

---

## USER GUIDE

***Version 1.0.0***

# Table of content

1. INTRODUCTION…….. 3

2. HOW IT WORKS…..…….. 6

3. HOW TO CONFIGURE…….. 7

# 1. INTRODUCTION

Antivirus Site Protection is the security extension to prevent/detect and remove malicious viruses and suspicious codes.

It detects: *backdoors, rootkits, trojan horses, worms, fraudtools, adware, spyware, hidden links, redirection and etc.*

Antivirus Site Protection scans not only theme files, it scans and analyzes all the files of your website (theme files, all the files of the modules, files in upload folder and etc).

> *This extension will be especially useful for everybody who downloads themes and modules from torrents and websites with free stuff instead of purchase the original copies from the developers. You will be shocked, how many free gifts they have inside.*

## Main features:

- Deep scan of every file on your website;
- Daily update of the virus database;
- Heuristic Logic feature;
- Quarantine & Malware removal feature;
- Alerts and Notifications in admin area and by email;
- Daily cron feature;
- Scanner can detect a wide list of malware types;

- Whitelist solution after manual review;
- Possibility to upload suspicious files to www.siteguarding.com server for review by experts;
- View Security reports online.

*Protect your website before the problems come. Monitor your website and minimize incident time with our automated scans.*

Antivirus Site Protection extension is a great solution for all website owners. It was developed by our engineers who has a many years experience in website security. Our extension intelligently crawl your website and identify all possible infections and backdoors on your website. Every day we update database and add new logics and functions (Heuristic Logic feature) to keep your website safe.

## The list of malware types what scanner can detect:

- **MySQL and JavaScript injections** (There is a lot of different attacks on your website but the most popular type and the easiest is probably MySQL injection. Our scanner will help you detect all possible issues with JavaScript and MySQL);
- **Website Defacements** (When hackers break in to your website they can change the appearance of your website or a webpage. We have set up a feature that can help you prevent any changes on your website);

- **Hidden iFrames** (If hacker gets an access to your website FTP they usually set up a hidden iFrame. That way they can use your website to get the viruses on your visitors computers);
- **PHP Mailers** (Sometimes hackers use your website to send a SPAM emails from your web server. Our smart scanning extension was made to detect all possible PHP mailing scripts on your website and prevent your website from sending SPAM);
- **Social Engineering Attacks** (There are a lot of social engineering methods to get an access to your website. Our scanning software will help you to protect your website);
- **Phishing Page Detection** (Hackers can install a phishing page on your website without you knowing it. Sometimes they can use your website);
- **Redirects**;
- **Website Backdoors** (Allow to get full control on website and server);
- **Website Anomalies**;
- **Drive-by-Downloads**;
- **Cross Site Scripting** (XSS);
- **.htaccess** (Hack Detection);
- **Rootkitsand** variants of this type of malware;
- **Trojan horses**;
- **Internet worms**;
- **Fraudtools**;
- **Adware** and **spyware** scrips and much more…

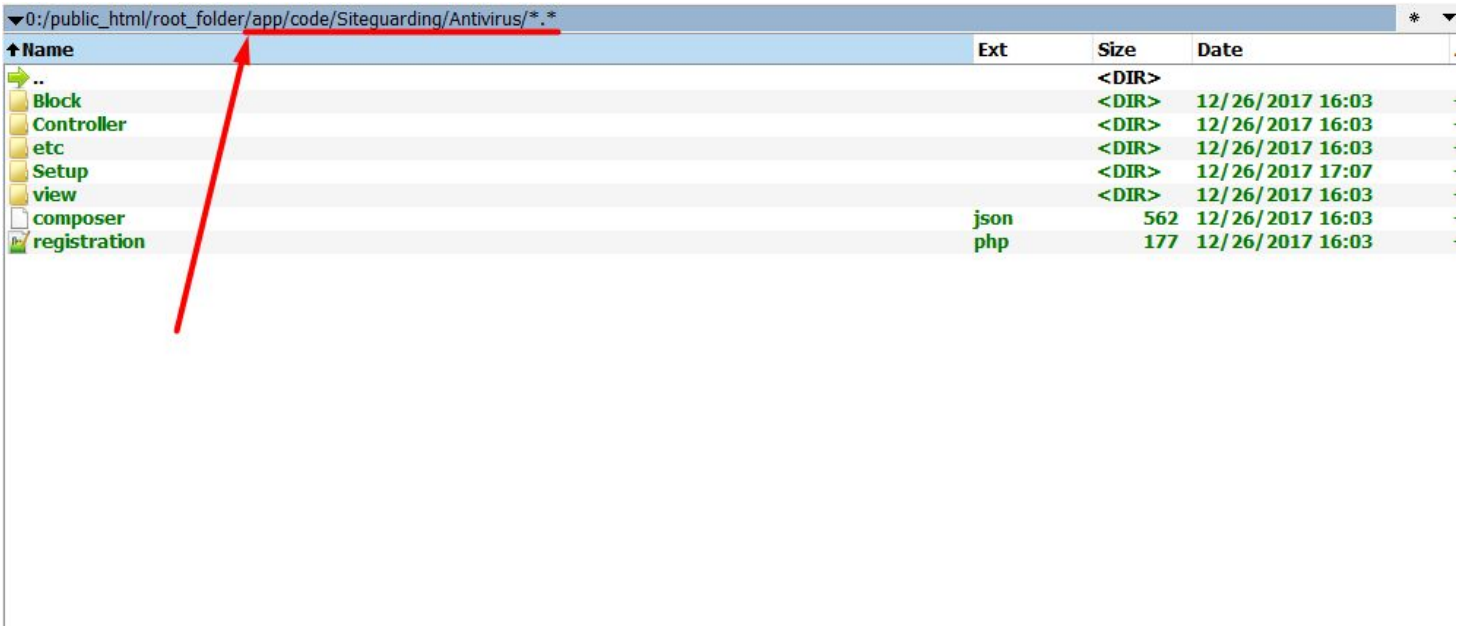
# 2. HOW IT WORKS

1. Registration. To communicate with SiteGuarding API, your website has to get session access key. Extension sends information about your website (domain and email) to SiteGuarding server. After successful registration your website will get unique access key. Please note: This action requires your permission and confirmation (nothing will be sent to SiteGuarding server without your permission).

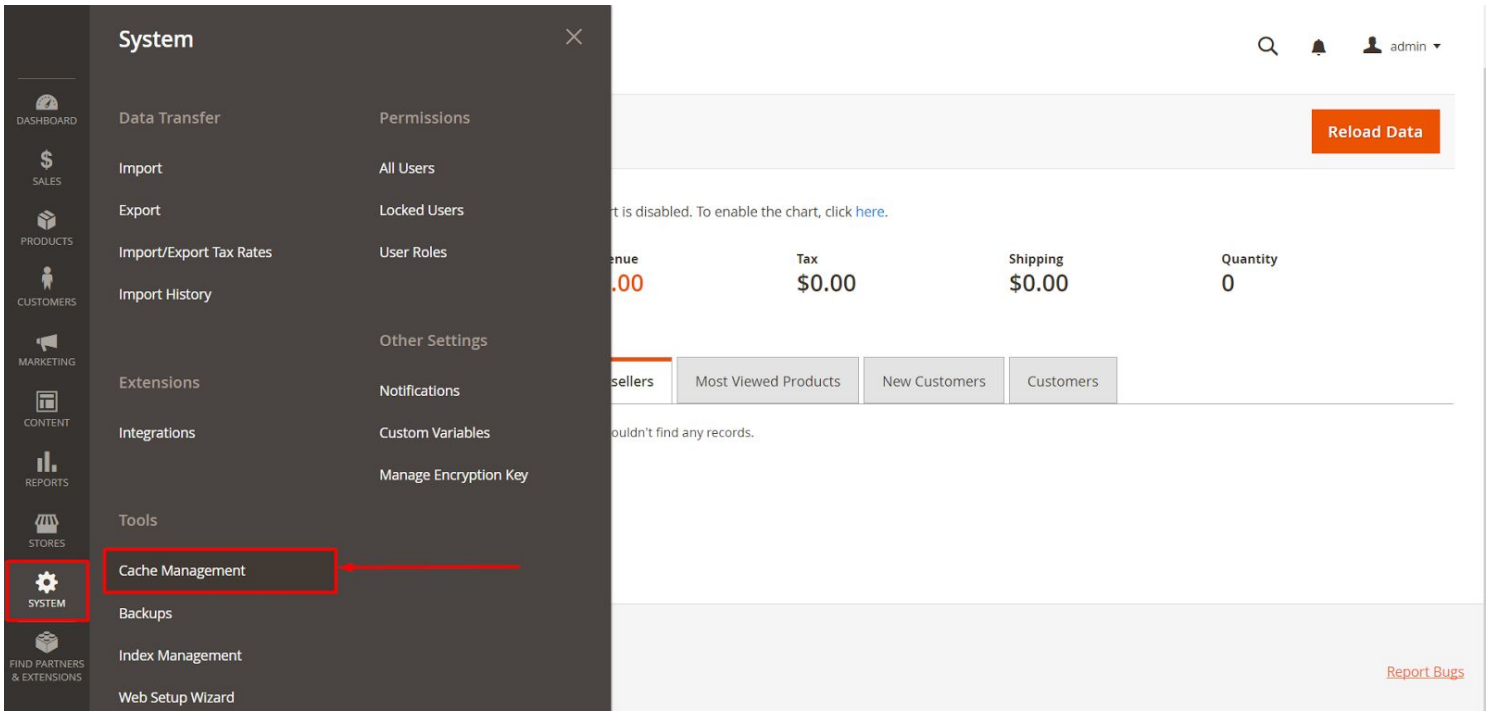
2. Scan process. During the scanning process, extension will read all the files of your website and will analyze them. Information about the files with suspicious codes will be sent to SiteGuarding server for extra analyze and for report generation. Generated report will be sent back to you (the copy of the report you will get by email). *Please note:* Extension sends and receives the data to SiteGuarding.com API.

# 3. HOW TO CONFIGURE

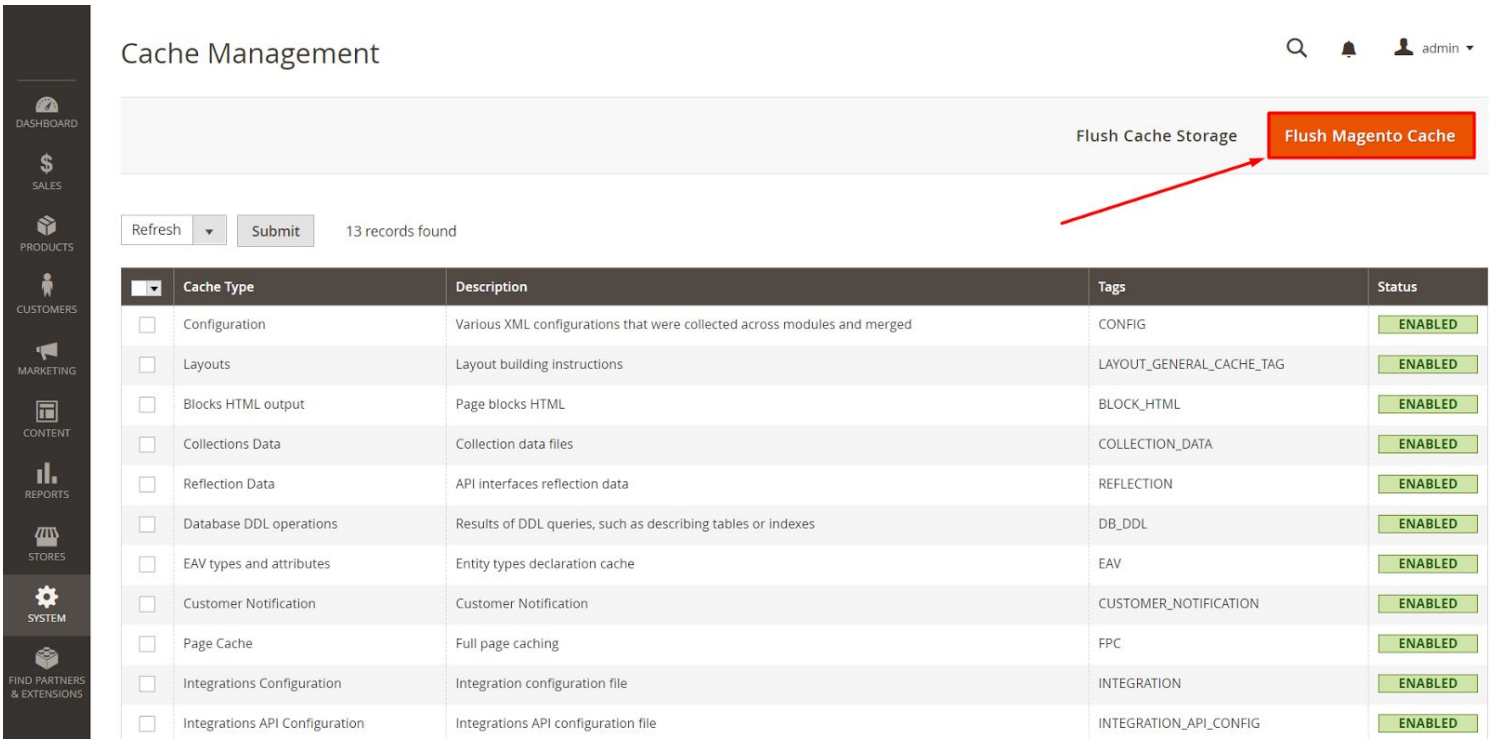
1. Go to the root folder of your website and in «app/code» create folder «Siteguarding». Set up permissions for this folder «755».
2. Here create folder «Antivirus». Set up permissions for this folder «755».
3. Copy files from the archive to directory «root_folder_of_your_website/app/code/Siteguarding/Antivirus».



4. Go to your Admin Panel → System → Cache Management:



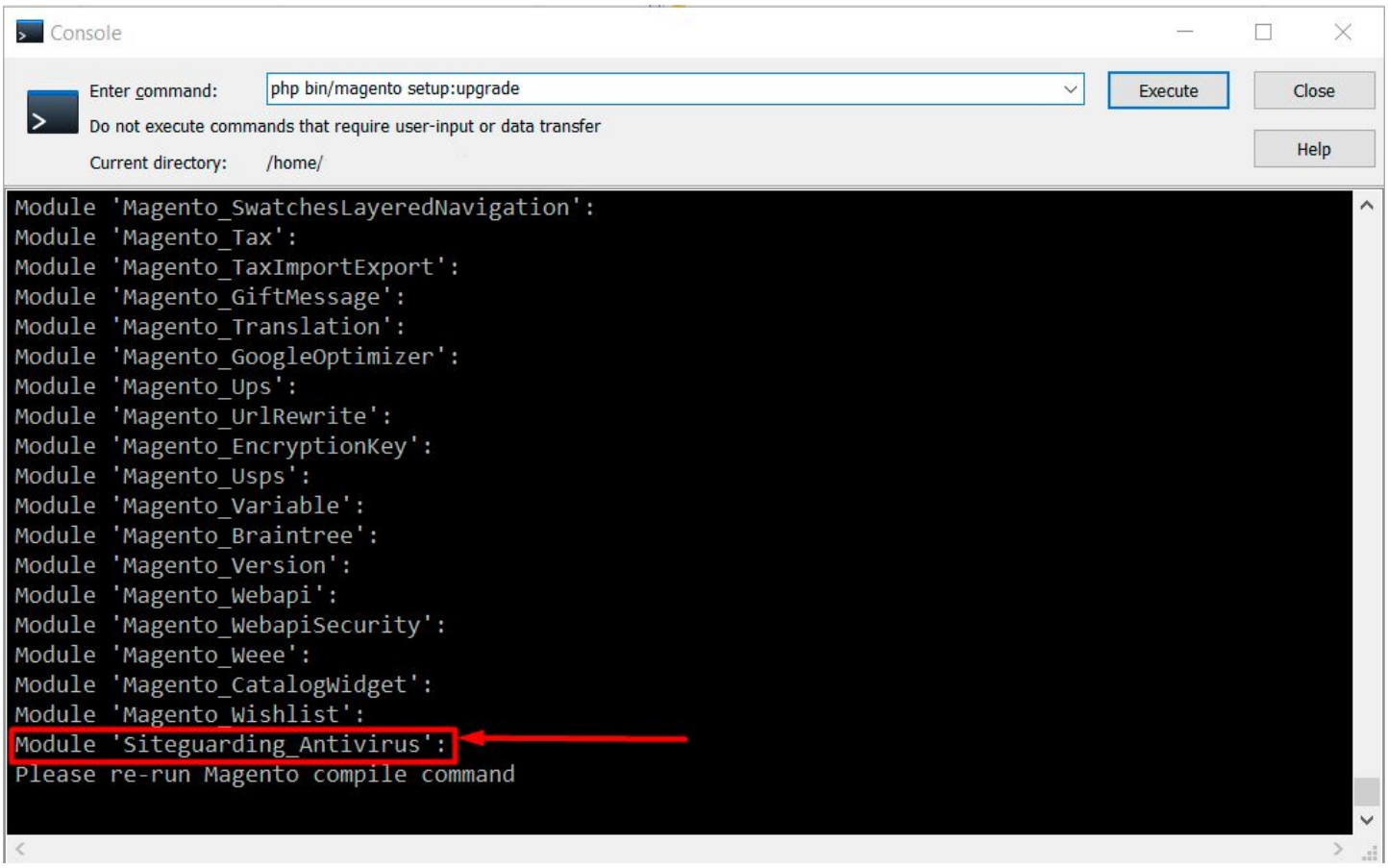
Click «Flush Magento Cache»:



5. To install extension you need an access to the server bash shell. Connect to your server by SSH and go to the root folder using next commands:

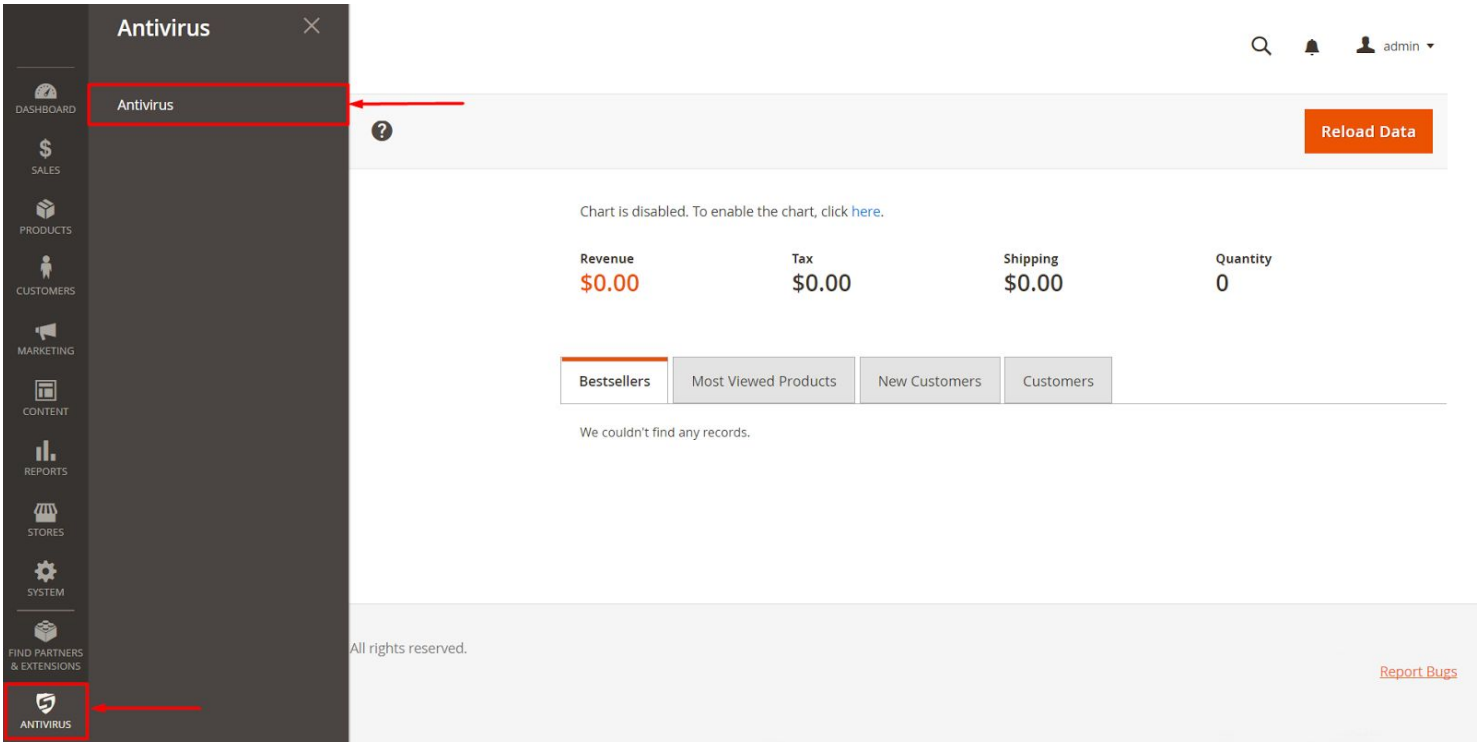
*cd «root_folder_of_your_website»/*

*php bin/magento setup:upgrade*

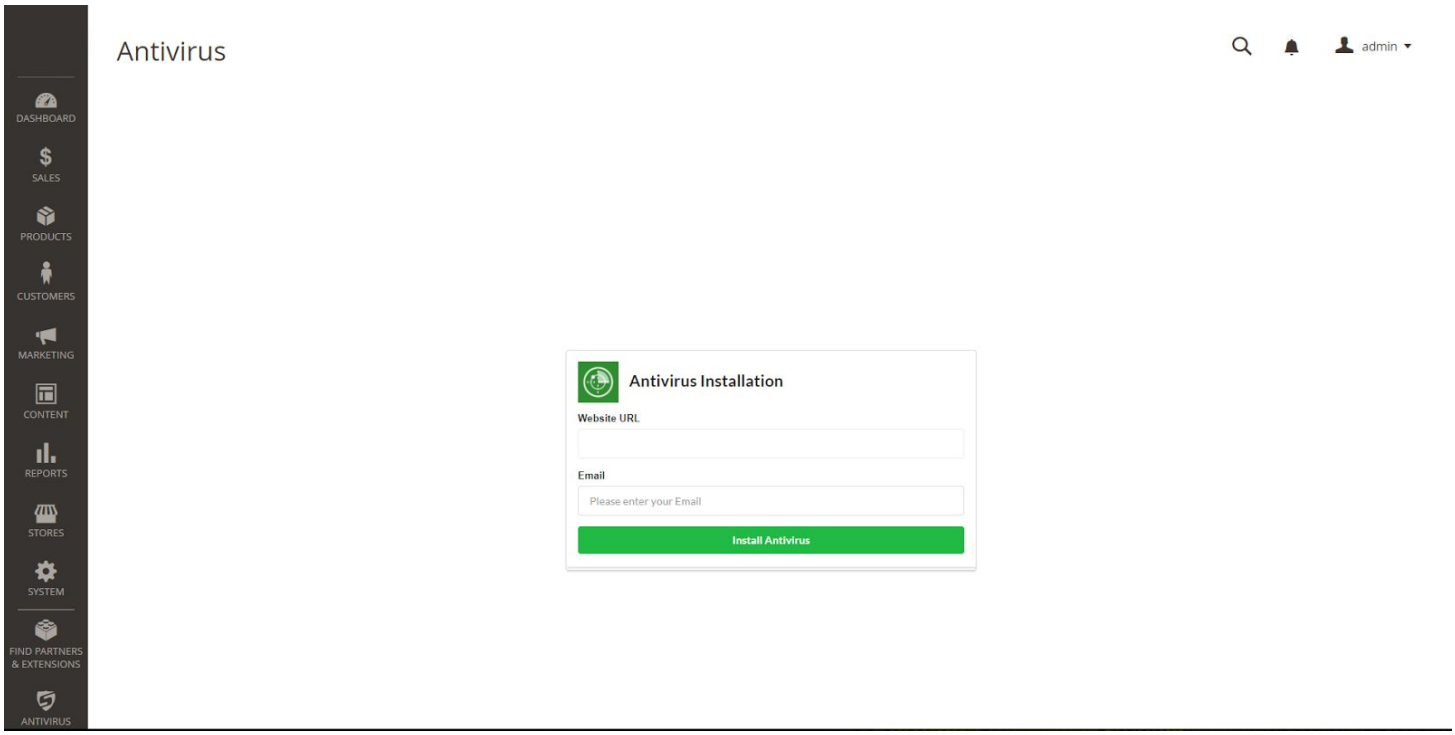



This command checks all of the modules and launches schema installation or updating process (if necessary). So you just need one command to perform updating and installation of all modules.

6. Go to Admin Panel and in the menu bar will appear tab «Antivirus». Click it and you will see the main page of the Antivirus:

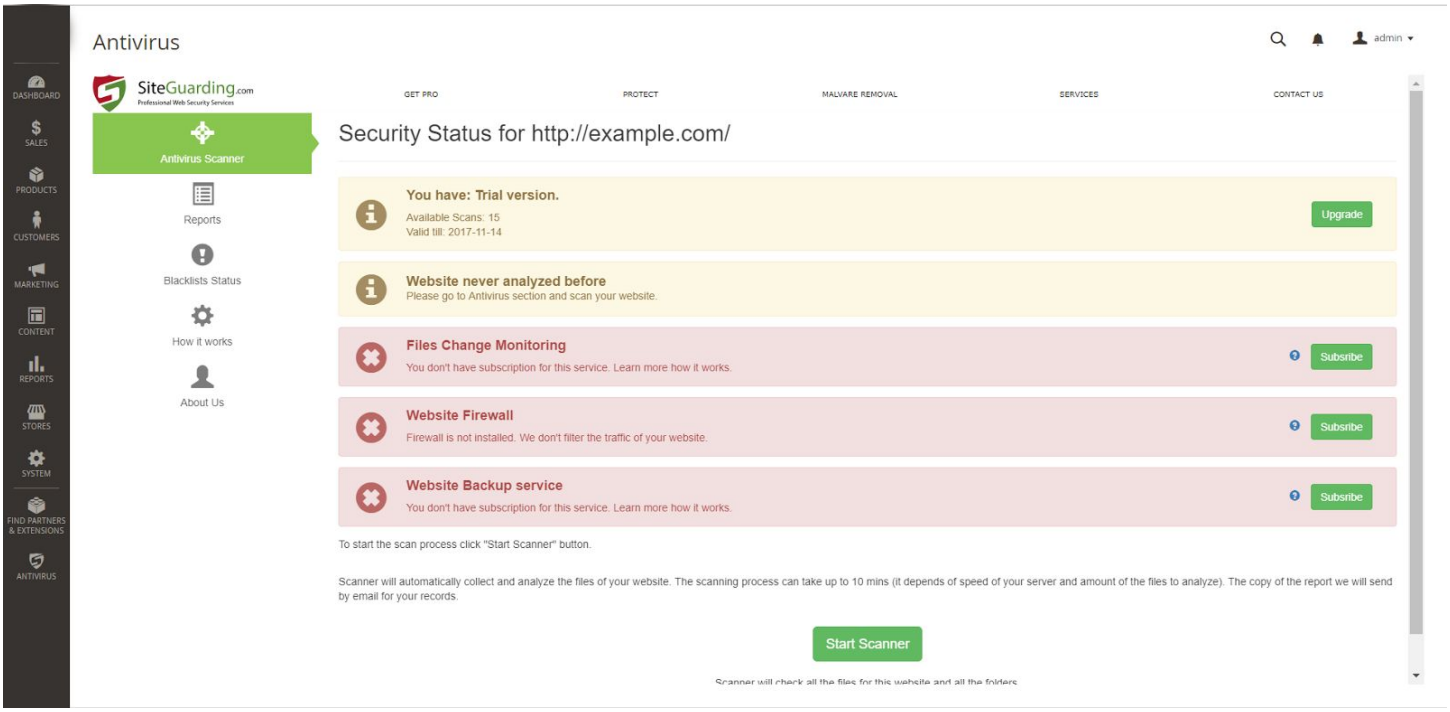


You will see the registration page.

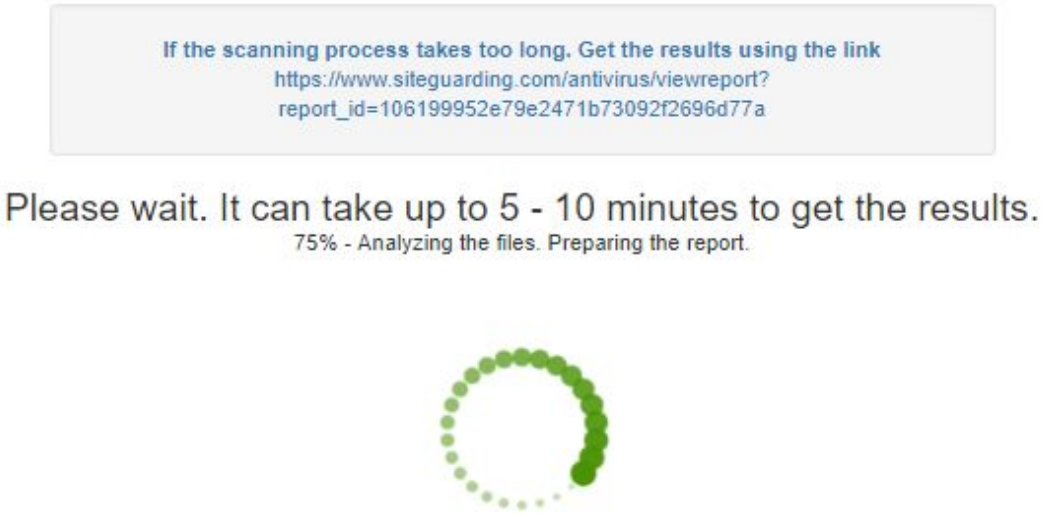



In the «Email» field, enter your email address to register your site and click «Install Antivirus».

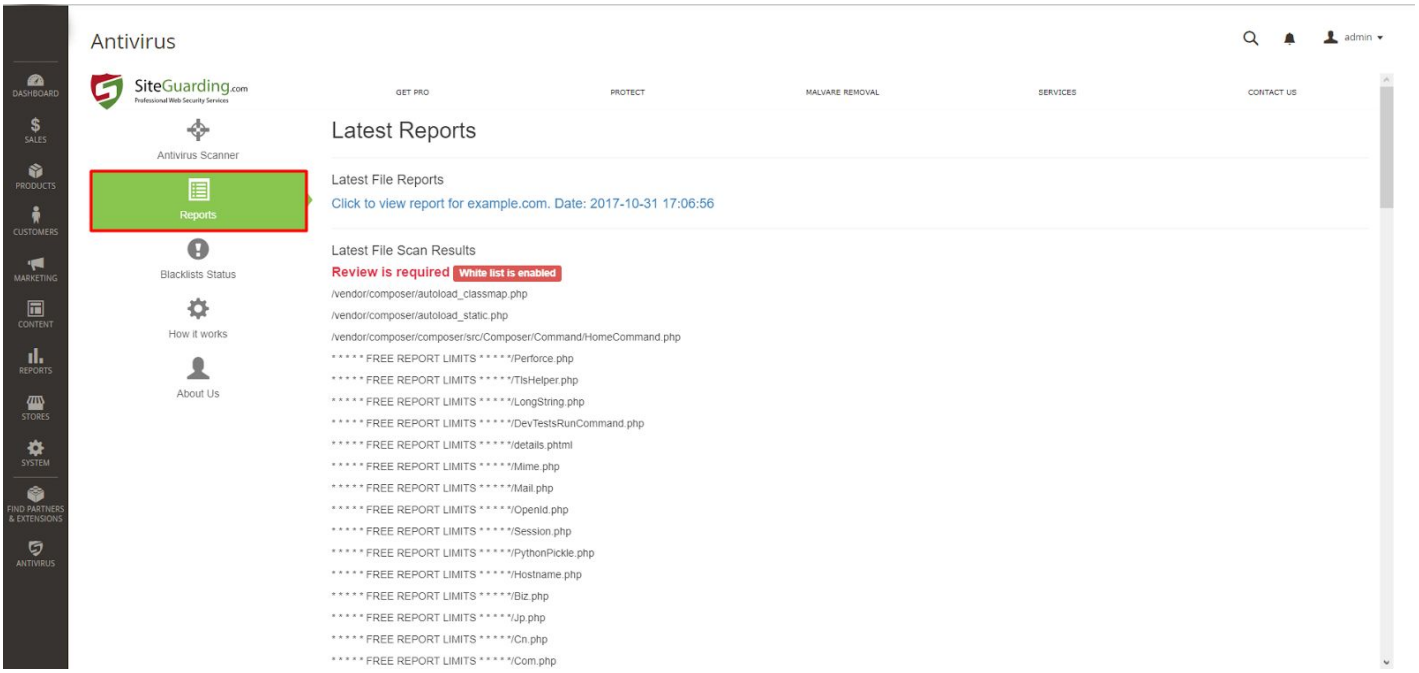
7. You will see the main page of the Antivirus:



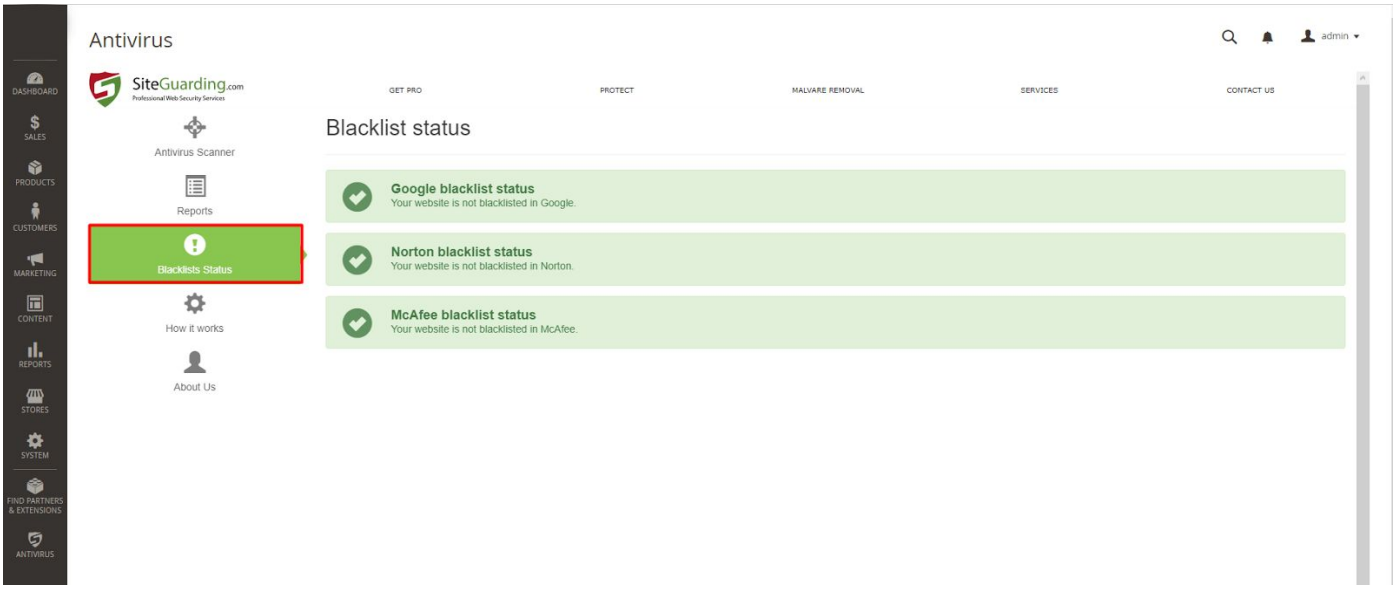

To start scan process click «Start Scanner» button and wait for the scanning process:



8. After scan process you will be redirected to the «Reports» tab. There will be list of suspicious files:



9. You can check blacklists status of your website in the «Blacklists Status» tab:




10. For additional services (get PRO version, clean website, website firewall, etc) use the «Antivirus Scanner» tab: